



FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

Egenevalueringsskjema

for foretakets elektroniske
overvåkningssystem mot
hvitvasking

Dato: 03.02.2009
Versjon 1.4

Finanstilsynet
Tlf. 22 93 98 00
post@finansilsynet.no
www.finanstilsynet.no

Evaluerings skjema for foretakets elektroniske overvåkningssystem mot hvitvasking

PO1	Etablering av elektronisk overvåkningssystem
PO2	Innhold i det elektroniske overvåkningssystemet – Kontroll mot FN's sanksjonsliste og FATF's liste over ikke-samarbeidende land (NCCT) ¹
PO3	Innhold i det elektroniske overvåkningssystemet - Flagging av transaksjoner
PO4	Oppfølging og administrasjon av det elektroniske overvåkningssystemet

Foretakets navn :

Dato :

Underskrift :

¹ NCCT = non-cooperative countries and territories

	PO1	Kontrollspørsmål		Kommentarer
	IT-Prosesser	Ja	Nei	
	Etablering av elektronisk overvåkningssystem			
	1. Har foretaket valgt verktøy for elektronisk overvåkning av transaksjoner? (Lovens § 15 ²)			
	2. Har foretaket etablert drift av system for elektronisk overvåkning av transaksjoner? (Lovens § 15)			
	3. Er kjøremønsteret for systemet for elektronisk overvåkning i samsvar med kjøremønsteret for betalingsformidlingstjenestene?			
	4. Omfatter overvåkningen alle typer transaksjoner ³ ?			
<u>Kommentarer:</u>				

² Lovens § 15. *Elektroniske overvåkningssystemer*

Rapporteringspliktige som nevnt i § 4 første ledd nr. 1, skal etablere elektroniske overvåkningssystemer. Departementet kan i forskrift gi nærmere regler om elektroniske overvåkningssystemer.

³ Unntatt interne transaksjoner eller overføring mellom egne konti i banken

		PO2		Kontroll- spørsmål	Kommentarer
IT-Prosesser		Ja	Nei		
<p>Innhold i det elektroniske overvåkningssystemet -</p> <p>Kontroll mot FN's sanksjonsliste og FATF's liste over ikke-samarbeidende land(NCCT) (Forskriftens § 10, første ledd ⁴, rundskriv 22/2003⁵)</p>					
<p>1. Bli navn på alle kundeforhold daglig kontrollert mot navn på personer og organisasjoner som står på FN's sanksjonsliste? ⁶</p>					
<p>2. Kontrolleres transaksjonens tekstfelt mot navn på personer og organisasjoner som står på FN's sanksjonsliste?</p>					
<p>3. Benyttes det fonetiske søk i navnekontrollen i punkt 1 og 2?</p>					

⁴ Forskriftens § 10 1. ledd *Undersøkelse av mistenkelige transaksjoner*

Forhold som kan utløse undersøkelsesplikt etter hvitvaskingsloven § 7 kan være at transaksjonen synes å mangle et legitimt formål, er usedvanlig stor eller kompleks, er uvanlig i forhold til kundens kjente forretningsmessige eller personlige transaksjoner, foretas til eller fra en kunde i et land eller område som ikke har tilfredsstillende tiltak mot hvitvasking eller terrorfinansiering, eller på annen måte har en uvanlig karakter

⁵ [Link til Finanstilsynets rundskriv 22/2003 "Håndtering av lister fra FN og FATF, samt lignende kunngjøringer":](http://www.Finanstilsynet.no/wbch3.exe?ce=11485)
<http://www.Finanstilsynet.no/wbch3.exe?ce=11485>

⁶ Link til FN's sanksjonsliste: <http://www.un.org/Docs/sc/committees/1267/1267ListEng.htm>

	4. Ved transaksjoner til eller fra utlandet, blir nasjonalitet på avsenders konto/mottakers konto kontrollert mot register over ikke-samarbeidende land i henhold til FATF sin liste (NCCT)? (rundskriv 9 / 2004 s. 25) ⁷			
	5. Blir listene det gjøres kontroll mot i punkt 1,2 og 4 daglig avsjekket mot kilden for listene?			
<u>Kommentarer:</u>				

⁷ Rundskriv 9/2004 s. 25

Transaksjonen foretas til eller fra en kunde i et land eller område som ikke har tilfredsstillende tiltak mot hvitvasking eller terrorfinansiering.

Her må særlig aktsomhet vises i forhold til transaksjoner utenfor FATF-området. Det er grunn til å være særlig observante overfor transaksjoner med kunder eller institusjoner i land med strenge sekretessebestemmelser, som tilbyr høy avkastning og skattefritak. FATF har også på sitt nettsted, www.fatf-gafi.org under overskriften "NCCT Initiative" en oversikt med nyttig bakgrunnsinformasjon om tiltak mot land og områder, som ikke samarbeider i kampen mot hvitvasking og terrorfinansiering ("Non Cooperative Countries and Territories"). FATF publiserer også en liste med oversikt over slike land og territorier. Endringer i denne listen publiseres også på Finanstilsynets nettsted. Hvitvaskingsansvarlig hos rapporteringspliktige må således jevnlig følge med på Finanstilsynets nettsted for å oppdatere seg på dette området. Det vises her også til Finanstilsynets rundskriv 22/2003 "Håndtering av lister fra FN og FATF, samt lignende kunngjøringer – endret praksis fra Finanstilsynets side", datert 29. august 2003.

Link til FATF sin liste: http://www.fatf-gafi.org/document/4/0,2340,en_32250379_32236992_33916420_1_1_1_1.00.html

	PO3		Kontroll- spørsmål		Kommentarer
	IT-Prosesser		Ja	Nei	
	Innhold i det elektroniske overvåkningssystemet - Flagging av transaksjoner				

	<p>1. Er reglene for flagging av transaksjoner i det elektroniske overvåkningssystemet dokumentert og fastsatt av foretaket?</p> <p>(For eksempler se forskriftens §10 første ledd og rundskriv 9/2004 s. 24 og 25⁸)</p>			
	<p>2. Er det etablert rutiner i foretaket for regelmessig evaluering av reglene for flagging av transaksjoner i det elektroniske overvåkningssystemet?</p> <p>(For eksempler se forskriftens §10 første ledd og rundskriv 9/2004 s. 24 og 25)</p>			

⁸ Forskriftens § 10 første ledd *Undersøkelse av mistenkelige transaksjoner*

Forhold som kan utløse undersøkelsesplikt etter hvitvaskingsloven § 7 kan være at transaksjonen synes å mangle et legitimt formål, er usedvanlig stor eller kompleks, er uvanlig i forhold til kundens kjente forretningsmessige eller personlige transaksjoner, foretas til eller fra en kunde i et land eller område som ikke har tilfredsstillende tiltak mot hvitvasking eller terrorfinansiering, eller på annen måte har en uvanlig karakter. ’

Rundskriv 9/2004 s. 24 og 25

Forskriften inneholder ikke noen definisjon på hva som er en ”mistenkelig transaksjon”. I forskriftens § 10 første ledd er det gitt anvisning på diverse forhold som kan utløse plikten til å foreta nærmere undersøkelser. Oversikten i det følgende er ikke uttømmende.

•**Transaksjonen synes å mangle et legitimt formål.**

Det kan eksempelvis være et oppdrag hvor pengesummen skal gå frem og tilbake mellom ulike konti innen en gitt tidsramme, at samme beløp går frem og tilbake mellom ulike institusjoner iht. et gitt oppdrag, og at en større sum splittes i flere mindre summer, men samles igjen på en ny konto.

•**Transaksjonen er usedvanlig stor eller kompleks, eller er uvanlig i forhold til kundens kjente forretningsmessige eller personlige transaksjoner.**

Det blir her tale om et konkret skjønn. En transaksjon kan være stor i forhold til én kunde, mens den er helt normal i forhold til en annen. Institusjonene må her nytte sine kunnskaper om den enkelte kunde. ”Kjenn-din-kunde”-prinsippet inngår her som helt sentralt.

•**Transaksjonen foretas til eller fra en kunde i et land eller område som ikke har tilfredsstillende tiltak mot hvitvasking eller terrorfinansiering** → ref. fotnote 7

•**Transaksjonen på annen måte har en uvanlig karakter.**

Det blir her tale om et konkret skjønn. Som eksempler nevnes:

- Rask og ekstraordinær nedbetaling av lån med kontanter
- Dersom det er et vesentlig misforhold mellom dokumentert betjeningsevne (inntekter, formue mv.) og lånebeløpet samt avtalte nedbetalingsbetingelser (ekstraordinær nedbetaling), kan det være en indikasjon på hvitvasking.
- Bruk av bankremitter som stadig blir fornyet
- Større vekslingsoperasjoner når gamle pengesedler blir ugyldige
- Bruk av ukurante betalingsmidler i forhold til den underliggende operasjon
- Store kontanttransaksjoner
- Bruk av betalingskort, hvor uvanlig mange store transaksjoner finner sted over et kort tidsrom

Et område som er særlig utsatt for hvitvasking og terrorfinansiering, er valutavirksomhet. Slik virksomhet omfatter valutaveksling og betalingsformidling mot utlandet. Det vises her til nærmere omtale på s. 54-64 i Ot.prp. nr. 81 (2002-2003).

De ovennevnte ”signalene” på mulig hvitvasking er ment som eksempler. Det er høyst sannsynlig flere eksempler. Dette er et område hvor det er stadig utvikling, og institusjonene må følge med og ta hensyn til nye trender og metoder i sine opplæringsprogrammer. FATFs hjemmeside på Internett inneholder her nyttig informasjon om slike tilfeller under overskriften ”Other Documents – Money Laundering Trends and Techniques”.

3. Reflekteres erfaringer fra manuell transaksjonskontroll i reglene for flagging av transaksjoner i det elektroniske overvåkningssystemet?			
4. Er systemet fleksibelt slik at regler kan endres, legges til og fjernes, terskelverdier oppdateres og profiler endres uavhengig av bistand fra leverandør av systemet?			
5. Gir systemet mulighet for at transaksjoner som av den elektroniske overvåkingen blir flagget som mistenkelige, fryses og unnlatt gjennomført inntil de er vurdert? (Lovens § 9 ⁹ , forskriftens § 14 ¹⁰)			
6. Dersom systemet inneholder funksjonalitet for å unnlate å gjennomføre flaggede transaksjoner, er denne funksjonaliteten tatt i bruk?			
7. Er brukergrensesnittet til systemet utformet slik at når en transaksjon blir flagget som mistenkelig, gir systemet informasjon om kunde og konto og andre transaksjoner knyttet til den berørte kontoen?			
8. Inneholder systemet funksjonalitet for automatisk generering av forventede verdier knyttet til ulike kontotyper/kundegrupper basert på transaksjonshistorikk?			
9. Dersom systemgenererte forventningsverdier blir benyttet, blir disse regelmessig oppdatert med utgangspunkt i en angitt periode med transaksjonshistorikk?			

⁹ § 9. Om gjennomføring av mistenkelige transaksjoner

Rapporteringspliktige skal ikke gjennomføre transaksjoner som medfører undersøkelsesplikt, før ØKOKRIM er underrettet. ØKOKRIM kan i særlige tilfeller gi pålegg om ikke å gjennomføre en slik transaksjon.

¹⁰ § 14. Forbud eller restriksjoner for rapporteringspliktiges adgang til å etablere kundeforhold med eller foreta transaksjoner til eller fra land som ikke har gjennomført tilfredsstillende hvitvaskingstiltak mv.

Finansdepartementet kan etter vedtak fra Financial Action Task Force on Money Laundering (FATF) fastsette særskilte forbud eller restriksjoner når det gjelder adgangen for rapporteringspliktige til å etablere kundeforhold med eller foreta transaksjoner med personer eller foretak som har tilknytning til land eller områder som ikke har gjennomført tilfredsstillende tiltak mot hvitvasking av utbytte fra straffbare handlinger eller forhold som rammes av straffeloven § 147a og § 147b.

Kommentarer:

		PO4		Kontroll- spørsmål	Kommentarer
IT-Prosesser		Ja	Nei		
Oppfølging og administrasjon av det elektroniske overvåkningssystemet.					
1. Er det utpekt en egen person eller avdeling med ansvar for daglig oppfølging av det elektroniske overvåkningssystemet? (Forskriftens § 10 fjerde ledd ¹¹)					
2. Rapporterer den som er ansvarlig for det elektroniske overvåkningssystemet til den i ledelsen som er ansvarlig for hvitvaskingsrutinene? (Lovens § 13 ¹²)					
3. Er det etablert dokumenterte rutiner for å daglig kontrollere resultatet av den elektroniske overvåkingen? (rundskriv 9/2004 s. 28 andre ledd ¹³)					

¹¹ Forskriftens § 10 fjerde ledd *Undersøkelse av mistenkelige transaksjoner*

Rapporteringspliktige skal etablere forsvarlige interne kontroll- og kommunikasjonsrutiner som sikrer oppfyllelse av undersøkelsesplikten. Det skal utarbeides interne rapporteringssystemer der ansatte som får mistanke som nevnt i første ledd, pålegges å rapportere til sin foresatte og til en hos den rapporteringspliktige særlig oppnevnt person eller avdeling. Denne personen eller avdelingen skal være direkte underlagt en særskilt utpekt person på ledernivå, som skal påse at kontroll- og kommunikasjonsrutiner er etablert og at rutinene følges når det foreligger mistenkelige transaksjoner.

¹² Lovens § 13. *Kontroll- og kommunikasjonsrutiner*

Rapporteringspliktige skal etablere forsvarlige interne kontroll- og kommunikasjonsrutiner som sikrer oppfyllelse av pliktene som pålegges rapporteringspliktige etter loven og bestemmelser fastsatt i medhold av loven. Kontroll- og kommunikasjonsrutinene skal være skriftlige og fastsatt på øverste nivå hos den rapporteringspliktige. Det skal utpekes en person i ledelsen som skal ha et særskilt ansvar for å følge opp rutinene. Det skal gjennomføres opplæringsprogrammer og oppfølging for ansatte og andre personer som utfører oppgaver til oppfyllelse av plikter etter loven.

¹³ Rundskriv 9/2004 s. 28 andre ledd

De transaksjonene som slike systemer identifiserer, må kontrolleres og følges opp manuelt før de eventuelt rapporteres til ØKOKRIM. Et elektronisk overvåkningssystem er et hjelpemiddel for å oppdage mulige mistenkelige transaksjoner. Uavhengig av slike systemer har rapporteringspliktige, deres ansatte, og andre personer som foretaket anvender i slike funksjoner, en selvstendig plikt til å undersøke mistenkelige transaksjoner, og for øvrig opptre i samsvar med hvitvaskingsregelverket.

	4. Er det i systemet for elektronisk overvåkning etablert autorisasjonsnivåer for å kunne skille mellom hvilke brukere som har lov til å betjene hvilke deler av systemet?			
	5. Er det laget rutiner for hvordan implementering av regelendringer i systemet, som nevnt i P03 punkt 4, skal kontrolleres og dokumenteres?			
	6. Inneholder systemet for elektronisk overvåkning funksjonalitet for arkivering av transaksjoner som er blitt underlagt intern behandling på grunn av mistanke om uvanlige forhold? (Lovens § 8 andre ledd og forskriftens § 10 femte ledd ¹⁴)			
	7. Inneholder systemet for elektronisk overvåkning funksjonalitet for sletting av transaksjoner som er oppbevart i 5 år? (Lovens § 8 tredje ledd ¹⁵)			
	8. Dersom transaksjoner blir elektronisk overført til Økokrim, blir disse kryptert eller på annen måte sikret mot innsyn? (Forskriftens § 11 tredje ledd ¹⁶)			

Lovens § 8 andre ledd

Rapporteringspliktige skal oppbevare dokumenter i tilknytning til transaksjoner som nevnt i § 7 første ledd i fem år etter at transaksjonen er gjennomført.

Forskriftens § 10 femte ledd

Rapportering internt i et foretak som ikke resulterer i rapportering til ØKOKRIM skal i dokument form være tilgjengelig i foretaket i minst fem år etter at rapporten ble mottatt av hvitvaskingsansvarlig.

¹⁵ **Lovens § 8 tredje ledd**

Dokumenter og opplysninger som rapporteringspliktige oppbevarer etter første og annet ledd, skal slettes innen ett år etter at oppbevaringsplikten opphører.

¹⁶ **Forskriftens § 11 tredje ledd**

Oversendelse av opplysninger skal skje ved bruk av standardisert formular fastsatt eller godkjent av ØKOKRIM. Oversendelse kan skje med post, telefaks eller i maskinlesbar form (elektronisk medium). Opplysninger som overføres elektronisk ved hjelp av overføringsmedium utenfor den behandlingsansvarliges fysiske kontroll, skal krypteres eller sikres på annen måte når konfidensialitet er nødvendig.